Multi-Domain Operations Workshop
2022 Technical Program

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 1 **JETS: EW T&E Capabilities Enabling MDO** **CUI: Distribution C**
Chair Geoff Wilson, T&E/S&T PM, Test Resource Management Center (TRMC)

2:45 p.m. **"Joint Electronic Warfare T&E Strategy"**
Geoff Wilson, T&E/S&T PM, TRMC

The purpose of the Test Resource Management Center (TRMC) Joint Electronic Warfare (EW) T&E Study (JETS) effort was to assess critical gaps and shortfalls in today's Joint EW T&E capabilities across the Services. The study focused on the adequacy of EW threat environment representations in the Airborne Electronic Attack domain. Advancing near-peer/peer EW threat capabilities are becoming increasingly adaptive, agile, and integrated, and the DoD test infrastructure must be improved to adapt and provide more complex EW threat T&E capabilities. Properly replicating the battlespace complexity and threat density can be a challenge in the EW T&E infrastructure; today's test infrastructure can replicate and test EW platforms within One-Versus-One environments, but is challenged with Several-Versus-Several test environments. The recommended JETS investment enhancements will enable more aircraft, both manned and unmanned, to test and train in a complex, realistic threat environments, including networked ranges and secure facilities, and at the scale and densities representative of "late 2020s" threat laydowns.

3:15 p.m. **"Open-Air Battle Shaping"**
Scott Weed & Rick Shelley, TRMC

Open Air Battle Shaping (OABS) is an air warfare concept that refers to providing a more realistic air warfare battlespace environment for advanced systems including, but not limited to, 4th and 5th Generation and beyond fighter and tactical and global strike aircraft. OABS the next logical evolution of the current air-to-air range instrumentation and air warfare battle shaping capabilities of the west coast test and training ranges, which are currently limited to specific aircraft and near-end of life aircraft instrumentation systems. OABS will integrate a wider range of Air Force and Navy aircraft and instrumentation systems, as well as improve the ability to perform large force air warfare test and training missions with simulated effects including Red and Blue weapons modeling, weapon scoring, and kill removal. The standardization and interoperability objectives of OABS will enable large force air warfare capabilities to be implemented and used at additional DoD test and training ranges. OABS enables Multi-Domain Operation assessments by integrating multiple ranges to enlarge the "playbox" and support more complex live or simulated effects during air warfare missions.

3:45 p.m **"Knowledge Management/Big Data Analysis"**
Billy Williams & Gene Hudgins, KBR

TRMC Enterprise Big Data Analytics (BDA) and Knowledge Management (BDKM) provides the capability to improve acquisition efficiency, keep up with the rapid pace of acquisition technological advancement, ensure that effective weapon systems are delivered to warfighters at the speed of relevance, and enable T&E analysts across the acquisition lifecycle to make better and faster decisions using data that was previously inaccessible or unusable. BDA is the application of advanced tools and techniques to help quickly process, visualize, understand, and report on data. The Joint Mission Environment Test Capability (JMETC) has demonstrated that applying enterprise-distributed BDA tools and techniques to T&E leads to faster and more informed decision-making that reduces overall program cost and risk.

4:15 p.m. **"Advanced Multi-Variate Time Series Analytic Techniques using AI & ML"**
Kenny Sanchez, TRMC; Tony Triolo, Perspecta Labs; Kathy Smith & Bill Wolfe, GBL Systems; Kent Pickett, MITRE

The goal of ATTENDS (Advanced Multi-Variate Time Series Analytic Techniques) is to provide advanced statistical analytic techniques that will allow analysts to make better/faster decisions by using multi-variate time series analytic techniques on data that was previously inaccessible or unusable, thereby gaining new insights. Instead of analyzing small chunks of data, the ATTENDS tools can give the analyst a broad view of the system, allowing the discovery of "unknown unknowns"; and provide alerts to analysts to find hidden problems. To achieve this goal, the ATTENDS architecture will be built with the following main goals:

- *Building a system to automate the process of ingesting a large amount of time-series data for analysis*
- *Developing state-of-the-art AI/ML models and algorithms that are suitable for targeted test use case applications*
- *Building a user interface that allows experts to submit queries related to specific applications*

Results from the ATTENDS analysis will be exposed to other C4T systems via the Cloud Hybrid Edge-to-Enterprise Evaluation & Test Analysis Suite (CHEETAS) interface.

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 2 **Mission Based Cyber Risk Assessment and Data Acquisition for MDO T&E**
Chair Kenny Hill, Business Development & Program Manager, Trideum

2:45 p.m. **"Data Acquisition System (DAS)"**
Jason Martin, Senior Solutions Architect, Trideum

The Data Acquisition System (DAS) product is an easily reconfigurable data collection, processing, and streaming system tailored to meet the data collection demands of low-cost, small form factor system-level testing. With a projected cost of under $15,000 per unit, a size of approximately 4"x4"x2.5", and a weight of < two (2) pounds, it brings powerful data collection capability into a size and form factor compatible with the most demanding environments. The DAS offers a combination of essential features into its own chassis, but also allows for the connection of modular peripherals which expand its capabilities based upon the requirements of the test. Best of all, it is more than just a data acquisition system; it is also a powerful and rugged miniature supercomputer with advanced data processing and machine learning capabilities. The DAS combines a powerful embedded computational platform, streaming and recording technologies, fast and reconfigurable wireless capabilities, and an array of attachable sensors and peripherals. It is easily configuring, deploys and operates via a wide array of power supplies, including batteries. At a typical "full load" power draw of less than 20W, batteries for up to two (2) hours of constant data collection are still practical in size.

3:15 p.m. **"Leopard"**
Jason Martin, Senior Solutions Architect, Trideum

Leopard designs bring a high degree of situational awareness, control, and insight into test events conducted at Test & Evaluation ranges and facilities. The ability to integrate multiple data sources - and leverage that information to provide consistent, accurate, and useful information - is key to maximizing value of test events, and in turn provide maximum value to Test & Evaluation customers. The data generated by instrumentation, cameras, and other relevant data sources can be immense. A single test event may involve collecting data from large numbers of System Under Test (SUT) and other data sources, each providing Time/Space Position Information data, high resolution video, system bus traffic within the SUT, and other sensor inputs. This data can be overwhelming, especially if disparate systems are sending data in separate ways, using different timescales, and different formats.
Leopard designs fill this capability gap. It is a single solution that is scalable, intuitive, flexible, and provides an extensible data management and visualization platform designed from the ground up to provide real-time intelligence through critical insight to testers and event managers. Leopard provides data management and analytics extended from and powered by CloudHybrid Edge-to-Enterprise Evaluation & Test Analysis Suite, combined with intuitive visualizations to provide

users immediate and actionable insight. When paired with video distribution hardware such as the Galileo video wall systems from RGB Spectrum, it can even integrate with these systems to further customize and control the in-event visualization experience.

3:45 p.m **"Cybersecurity Vulnerability and Assessment Test Environment (CVATE)"**
Aaron Gould, Senior Solutions Architect, Trideum

The Cybersecurity Vulnerability and Assessment Test Environment (CVATE) Other Transaction Authority advances the Redstone Test Center (RTC) Distributed Test Control Center into a robust, repeatable, and instrumented environment to support the challenging need for cybersecurity vulnerability testing for U.S. Army weapon systems. CVATE leverages RTC resources and partner test organizations to provide Testing and Evaluation capability. CVATE developments go beyond compliance-based cyber assessments. CVATE consists of capabilities for assessing the effects of adversarial cyber operations at the subsystem, system, and system of system levels as well as at the mission level, while the test article merges in a representative mission environment.
As the foundation of the RTC's overall cyber–Developmental Test and Evaluation strategy, CVATE uses a realistic operational environment with simulation/stimulation as well as representative cyber threats based on the latest intelligence information. State-of-the-art instrumentation is available for high-speed and high-quality data collection, analysis, and visualization. Mission-impact from cyber threats reports and archives to inform cyber risk to Program Managers.

4:15 p.m. **"MDO Sensor to Shooter T&E"**
Ken LeSueur, Trideum

The Army Test and Evaluation Command (ATEC) lacks an end-to-end Live Virtual Constructive (LVC) test environment to assess Sensor to Shooter (STS) System of Systems (SoS) that is operationally relevant, has sufficient scale, and that is Verified, Validated, and Accredited (VV&A). The architecture proposed in this presentation supports the seamless switching of the STS component systems between 1) Digital Twin 2) Hardware-In-the-Loop (HWIL) and 3) live representation in the test environment. The capability shall allow scaling of the test environment from small, single thread STS chains to larger Brigade and Division scaled implementations, and finally, to support Multi-Domain Operation (MDO) test scenarios.

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 3 **Cyberspace Test Technology**
Chair Min Kim, Deputy Executing Agent, TRMC T&E/S&T Cyberspace Test Technology (CTT)

2:45 p.m. **"Measure and Share"**
Dr. Michael Shields, TRMC T&E/S&T CTT Chief Scientist, &
Pete Firey, MITRE

Current DoD Cyber testing is conducted in a stove piped and independent event manner resulting in testing inefficiency. There is no universal mechanism to quantify the efficacy of a cyber test, and mechanism to promulgate test results to the T&E community and the broader DoD community. The goals of this project is to develop an initial set of measurement tools that provide quantitative analysis of test events, and develop "perspectives" which provide the information that are domain (e.g., T&E perspective, Operational perspective, Acquisition perspective and Intel perspective) specific. This presentation provides a proposed solution to measure the efficacy of cyber test event and share the test results at an appropriate classification level.

3:15 p.m. **"Vader Modular Fuzzer: What, Why and How"**
Arch Owen, Program Manager, Draper

TRMC is developing "Vader Modular Fuzzer" to address the broad range of U. S. Government fuzzing needs. The Vader Modular Fuzzer is based on Draper's Vader modular software fuzzing framework. Its modularity permits fuzzing developers to quickly create new fuzzing capabilities by designing specialized modules and integrating those modules into the existing framework. Ongoing development is focusing on usability, enhanced modularity, application to embedded systems, and advanced fuzzing features. The Vader Modular Fuzzer will provide the DoD and other Government agencies an open source, modular, no-fee solution for fuzzing the critical software and systems.

3:45 p.m **"Automated Machine Learning for Cybersecurity"**
Dr. Himanshu Upadhyay, Florida International University, Principal Scientist

Florida International University in collaboration with Test Resource Management Center has developed Cyber Threat Automation and Monitoring (CTAM) system to detect, analyze and monitor the test vector behavior during cyberspace attacks in the virtualized environments. CTAM is designed to identify the impact of test vector on the specified mission using advanced instrumentation tools focused on smart memory acquisition with virtual memory introspection (VMI) and advanced cyber analytics using the state-of-the-art artificial intelligence methodologies. Team has developed an automated machine learning system using the AI based advanced analytics platform of the CTAM. This is a standalone system which allows machine

learning model building, advanced analytics and visualization of predictions using the data collected from different test technology domains using traditional machine learning / deep learning and ensemble learning approaches. This system has automated machine learning through various platforms like AI based Advanced Analytics, Analytics Control Center and Data Source platforms. This presentation will start with AI/ML basics and further discuss the AAML features.

4:15 p.m. **"Automated Attack Framework for Test & Evaluation (AAFT)"**
Andrew Shaffer & Bruce Einfalt, The Applied Research Laboratory,
The Pennsylvania State University Research and Development Engineer

Red Team cybersecurity testing is critically important to ensure that new systems will perform as expected without compromising mission success. Unfortunately, no individual Red Team can keep up with the torrent of new threats that are being discovered every day. Also, a lack of cybersecurity Red Team availability often delays system accreditation and forces procurement programs to move forward with less mission assurance than is desired.

The Automated Attack Framework for Test & Evaluation (AAFT) enables Red Teams to keep pace with the threat by providing a framework for Red Teams to collaboratively capture and share information about threat cyberattacks in a format that is intelligible to an autonomous cybersecurity testing system. It also improves Red Team utilization and efficiency by automating the execution of threat cyberattacks and emulating basic and intermediate-level cyber threats so that Red Teams can focus on emulating more sophisticated threats, increasing the overall scope of cybersecurity testing that can be performed.

The basic AAFT framework has now been implemented and a wide range of different cyberattacks have already been integrated for use in AAFT-enabled automated testing. Development of the AAFT system is ongoing, and plans are in place to scale up the complexity and scale of the attacks that AAFT can autonomously execute.

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 4 **T&E Methodologies and Approaches to Advance MDO**
Chair Gina Sigler, Scientific Test and Analysis Techniques (STAT) Center of Excellence (COE)

2:45 p.m. **"A Novel Concept for T&E of Autonomous Systems in Multi-Domain Operations"**
Charlie Middleton & Dr. Lenny Truett, Scientific Test and Analysis Techniques Center of Excellence

Not releasable

3:15 p.m. **"Applying STAT Concepts of Model Validation with Multiple Sources"**
Nick Jones & Kyle Provost, Scientific Test and Analysis Techniques Center of Excellence

The Department of Defense (DoD) currently faces rapidly changing operational environments and emerging threats that require complex engineered multi domain defense systems to be developed on ever-shorter timelines. To meet this need, the DoD is placing increasing trust in modeling and simulation (M&S) for the design, development, and engineering of new capabilities. Therefore, it is crucial that decision makers and developers understand whether models are valid and trustworthy representations of the systems under development. Validation is a process which determines the trustworthiness of a model by assessing whether the model has sufficient fidelity relative to an appropriate referent(s) for a specific intended use. Validation referents are needed to quantify fidelity: the level of consistency between a model and reality. However, validation is often complicated by the need to use multiple sources of information as referents for the true system behavior. These referents could include other more established models, more than one lab source, or even more than one live fire test event. Scientific Test and Analysis Techniques (STAT) provide the methods to quantify the fidelity. This brief will utilize a case study to delineate how to use STAT as the foundation for quantifying fidelity and account for differences in scope when validating models versus multiple referents.

3:45 p.m **"Applying Design of Experiments (DOE) to Testing and Evaluating Performance Across the Cyber Domain"**
Dr. John Hong, Institute for Defense Analyses, Assistant Director

The core of the emerging National Defense Strategy will include "integrated deterrence,… a framework for working across warfighting domains, theaters and the spectrum of conflict." Thus, successfully executing Multi-Domain Operations (MDO) will remain key to the strategy. Enabling successful execution will include resilient performance across the Cyber Domain, an important and increasingly

contested part of MDO. Comprehensive and efficient cybersecurity testing will be needed to rigorously evaluate the resilience of performance across the Cyber Domain. It has become standard practice to use Design of Experiments/Scientific Test and Analysis Techniques (DOE/STAT) to develop efficient tests and evaluate their results without considering every of the many combinations of factors that can affect system performance. This approach has been widely applied to conduct both developmental and operational testing outside the Cyber Domain. This presentation demonstrates how DOE could be applied to support efficient and rigorous cybersecurity testing and evaluation.

4:15 p.m. **"Digital Engineering Enabling T&E Planning Through the Integrated Decision Support Key (IDSK)"**
Jean Petty & Suzanne Beers, PhD, MITRE

The Integrated Decision Support Key (IDSK) provides a framework for articulating cradle to grave lifecycle decision making, informed by an evaluation of both operational and technical capabilities, drawing data from the full test continuum of early contractor testing through full-up system of system operational test and/or modeling and simulation. Applying the IDSK thought process to multi-domain operations use cases could inform the effectiveness of the existing JADC2 reference architecture in meeting MDO mission objectives, guide the design of the campaign of experimentations and demonstrations to gather the data needed to evaluate architectural components' mission contributions, and inform system/architecture refinements to better accomplish mission objectives. This presentation will walk through the IDSK's evaluation-based decision support concept and illustrate its use with a notional MDO application.

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 5 **Multi-Domain Initiative**
Chair Hans Miller, Project Leader, OSD Programs, The MITRE Corporation

1:00 p.m. **"The All-Domain Test Range and the Family of Options"**
Michael Hesse, Principal, Systems Engineering, MITRE

Great Power competition requires both new hardware and new approaches if the United States and its warfighters are to maintain their edge. Test and evaluation (T&E) is no exception. T&E methodologies and infrastructure must merge seamlessly with an adaptive DoD that leverages the power of data, modelling, and simulation to create a recurring and increasing cycle of value for its decision makers. To maximize this value, this cycle should stretch from experimentation to initial operational testing to mission rehearsal training. Having plotted an immense and diverse space, this brief expands on how assessment must now expand and evolve to meet the challenging requirements of system of systems testing in a multi-domain environment while permitting stakeholders to select from a Family of Options empowering them to right-size and right-time assessment opportunities - and fuel timely, informed decision.

1:30 p.m. **"M&S as a Service: A Multi-fidelity On-Demand Hybrid Cloud-Enabled M&S Infrastructure to Exercise Family of Options"**
Dr. Saurabh Mittal, Principal Scientist and Project Leader AFLCMC/XA, MITRE

The Department of Defense is expected to increase their use of synthetic, operationally representative simulation environments to support the design and testing of advanced, next-generation aircraft and weapon systems. An integrated modeling and simulation (M&S) analytic workbench for Test and Evaluation (T&E) is needed to fully enable this vision. The increasing complexity of systems and reliance on information provided through collaboration between systems and services requires the use of digital tools, processes, and methods to capture data and data relationships among components in both static and dynamic forms. This requires the development of a common reference structure that ensures conceptual alignment of various models and emerging services, which unambiguously identifies information exchange requirements and supporting interfaces under the constraints of operational test scenarios. This briefing will describe the MITRE developed Simulation, Experimentation, Analytics and Test (SEAT) conceptual framework, a layered service-oriented reference architecture and its implementation as an on-demand cloud-enabled multi-fidelity M&S architecture for T&E in multi-domain environments. This presentation will showcase an Expedient Leader Follower (ExLF) use case and demonstrate how a distributed architecture integrates high-fidelity tools such as the Unreal Engine and customized autonomy controllers that govern Unreal entities externally using service interfaces. We will then explore how this framework can serve as one of a family of options to assess Multi-domain concepts and approaches.

2:00 p.m **“DARPA Stitches and its Application to T&E”**
Dr. Jimmy "Rev" Jones

TBD

2:30 p.m. **“Live Range Multi Domain T&E - Orange and Emerald Flag”**
Major Brandon "Siphon" Burfeind, 412th TW Director of Orange Flag and F-22 Test Pilot

TBD

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 6 **Leading to T&E Excellence**
Chair Richard Martinez, GreyBeards Group

1:00 p.m. **"Leading to T&E Excellence"**
Jason Farley, UTEP, College of Engineering, TMAC

Global security threats aren't just changing, they're adapting and they're doing it faster than ever… on all fronts! The diverse and rapidly evolving capabilities of our adversaries requires a defense and security response that is even more dynamic and comprehensive. As a part of that response, the Department of Defense organizes the development and fielding of solutions through the Defense Acquisition System. Great work has been achieved in modernizing that organization and its processes, including the Adaptive Acquisition Framework, the New 5000 Policies, MOSA, etc., that enable effective program management, facilitate agility, and enhance delivery capability to produce at the speed of relevance. A critical component of the DAS is Test and Evaluation. It is not enough for T&E to keep pace with other components of the DAS, it must be out in front! Said another way, it is required that the T&E function sustain performance excellence.

Test and Evaluation can be done better, no matter the current state. This statement represents a principle. Of course, there are many principles… literally countless. So, does this particular principle deserve to be prioritized and cultivated, perhaps even elevated into a value for organizational units working within the T&E for MDO enterprise? To wit, test and evaluation for MDO can be designed and developed to be precisely what is needed, delivering the most accurate and trustworthy results. It's a matter of how well the system is designed and executed. There are many disciplines at work in the enterprise of T&E for MDO: engineering, science, business management, etc. Subsequently, there are many associated approaches, models, and frameworks that can lead to the use of many more methods, techniques, and tools. The T&E for MDO enterprise presents a complex environment. Management has the daunting task of organizing, including continually developing and effectively using, a precisely focused T&E system that delivers on a value promise in pursuit of the third Imperative of Combat: "believe in your weapons and equipment".

How can management achieve operational excellence in T&E for MDO? Fundamentally, it begins with achieving organizational excellence and culminates in the validated delivery of value. The pursuit of excellence begins on a foundation of principles that drive behavior and decision-making. And yet, an enterprise does not always select or fully understand appropriate principles, that is principles of consequence. How does this happen if there are bodies of knowledge, supposed "best practices", and standards? The answer can be found in understanding the nature of the system of interest and scrutinizing the principles upon which the system is and should be designed and operated.

The T&E for MDO enterprise is a socio-technical, adaptive system of systems in which thousands of principles drive decisions every day. If the system is to be optimized, participants must be enabled and empowered to take informed action guided by appropriate principles, i.e., responsible and aligned agency as a building block for operational excellence. Competent leadership and management are critical in developing a value creation system and culture that are engaging and produce maximum value.

1:30 p.m. **"RTC Approach to Persistent Integrated Developmental (RAPID) Testing"**
TBD, PeopleTec

The RTC Approach to Persistent Integrated Developmental (RAPID) Testing effort provides a digital engineering-enabled distributed test collaborative environment for Army modernization programs. Support includes the following major task areas: model-based systems engineering, modeling and simulation, agile software development, hardware/software integration, cloud design, digital twin testing, SySML/Cameo customization, and DevOps/DevSecOps. RAPID is the development, integration and modernization of laboratory and open-air test environments, connected through distributed networking, utilizing new M&S resources to the greatest extent, and managed with processes based on a model-based systems engineering (MBSE) approach. The solution provides RTC the ability to test system compatibility, interoperability, standard conformance, and system performance at the component level up to full platform level in both a modeled (virtual) environment and with physical hardware in a simulated and an open-air environment. RAPID established the Mission Systems Test Capability, a SoS-focused lab that will account for current and future MDO aircraft configurations and integrate digital twins for MDO environment and MOSA conformance testing.

2:00 p.m **"TSA System-of-Systems Study to Support Integrated Test and Evaluation"**
Erick Rekstad, Transportation Security Administration (TSA)

The airport security checkpoint is TSA's predominant method for screening passengers and their carry-on possessions prior to boarding an aircraft. The checkpoint consists of a range of complementary technology areas, including Identity Verification, Accessible Property Screening, On-Person Screening, and Alarm Resolution. TSA is challenged to continuously improve screening capabilities to keep pace with the evolving threat landscape and maintain an understanding of the interconnectedness of checkpoint technologies to drive collective system performance. To address these challenges, TSA requires a modeling and simulation capability that can dynamically assess screening tradeoffs, integrate outcomes, and identify operational impacts throughout TSA's acquisition lifecycle. The purpose of the System-of-Systems (SoS) study is to leverage Digital Engineering practices and tools to model interactions, simulate scenarios, and analyze outcomes of a checkpoint with integrated processes, techniques, and technologies. The ultimate goal of the study is to ensure TSA is deploying optimized configurations of screening technology to airport checkpoints that maximize security effectiveness, passenger throughput, and reliability.

The SoS study utilizes a Model-based Systems Engineering (MBSE) approach to establish a baseline checkpoint model that simulates and analyzes user-defined

scenarios for specific checkpoint configurations. TSA will examine current and future checkpoint performance against existing requirements, review individual checkpoint constraints, and consider interdependencies across technology equipment. As TSA deploys thousands of equipment upgrades over the next 3-5 years, the SoS study will scale to support a diverse security technology marketplace. The robust analytics behind SoS modeling will inform checkpoint design now and into the future, allowing TSA to flex and surge as needs dictate.

The five key objectives of TSA's SoS study are to:

- *Optimize System Configurations by establishing optimal performance configurations and quantities for each screening technology based on the latest security, throughput, and reliability data to determine the overall checkpoint system operational capability.*
- *Mitigate Constraints by identifying checkpoint system performance constraints and proposing mitigation strategies.*
- *Characterize Systems and Allocate Resources by defining various checkpoint configurations and required staffing levels for each configuration increment.*
- *Maximize Modeling Components via reuse and incorporating the checkpoint model and its outputs across different screening programs.*
- *Enhance Analysis Collaboration by leveraging commercially available products to support modeling, simulation, and analysis that can be easily managed and integrated with other tools.*

Through collaboration with DHS's Systems Engineering & Standards and Operational T&E Divisions, TSA has completed the development of the initial SoS study model using the Systems Modeling Language (SysML) and is currently conducting an SoS study pilot to incorporate existing operational data into the model. The SoS study pilot will simulate multiple scenarios using recent field data to derive insights on model fidelity; checkpoint configuration throughput, security effectiveness, and reliability metrics; and allow for the comparing of different checkpoint screening configurations. The modeling analyses and optimization recommendations will inform SoS model improvement and requirements refinement while equipping TSA with the ability to dynamically assess the impacts of system design and configuration decisions for near-term acquisition and deployment events.

2:30 p.m. **"TBD"**
TBD

TBD

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 7 **Supporting and Enabling all the Domains for Operational Effect**
Chair Cedric Baca, C4ISR Division Chief, Army Futures Command (AFC), DEVCOM Analysis Center

1:00 p.m. **"Electromagnetic Warfare (EW) Threat Environments for Lab Based Risk Reduction (LBRR), Experimentation, and Testing"**
Cedric Baca, C4ISR Division Chief, Army Futures Command (AFC), DEVCOM Analysis Center

Provide an overview of the state of art Electromagnetic Warfare (EW) for open air experimentation and testing, laboratory experimentation, and EW assessments across the Electromagnetic Spectrum (EMS). Discuss the leading edge tools, techniques, and methodologies used to ensure electromagnetic spectrum dominance for the Warfighter.

1:30 p.m. **"Cyber Experimentation, Analysis & Assessment in Support of Army Modernization Enterprise"**
Humberto Mendoza, Army Futures Command (AFC), DEVCOM Analysis Center (DAC)

The cyber division from the DEVCOM Analysis Center (DAC) executes cyber experimentation & analyses in support of Army Modernization priorities, readiness programs, and acquisition T&E. DAC will provide an overview of cyber tools, techniques, and methodologies used to identify vulnerabilities and collaborate with Army PEOs/PMs to develop remediation solutions that enhance the cyber resilience of Army technologies. DAC will also provide overview of future development capabilities in distributed cyber experimentation and analysis, as well as capabilities in coordinated Cyber Electro-magnetic Activities (CEMA) techniques within an MDO environment.

2:00 p.m **"DevOps to DevSecOps: Making Security Part of Your Development Operations"**
Steve Seiden, President, Acquired Data Solutions

System developers are adopting continuous software delivery practices into the planning, build, test, release, and monitoring phases of product development. Networked systems, particularly those with embedded web servers, carry the additional burden of having to protect against security threats.

This presentation introduces best practices for adding automated security scanning, analysis, remediation, threat management and monitoring to continuous development processes. Adding automated testing to software build pipelines enables teams to secure their systems continuously in recurring build/test loops.

2:30 p.m. **"Supporting and Enabling all the Domains for Operational Effect"**
Colonel (USA, Ret) Joel Babbitt, Vice President for Army Programs, Viasat Government Systems

The conduct of war has grown exponentially more complex and requires mastery of land, sea, air, space, and cyberspace. The underpinnings of that mastery are a vast and complex array of highly technical capabilities that our warfighters must bring together for operational effect. What gives the U.S. military its dominant position in the world is not just its size, funding, and professionalism, but its relentless innovation in bringing together all the pieces of the symphony of war. This is especially true in targeting, where Link16, Cyber/FMV/other ISR, and communications capabilities come together to provide unprecedented speed and accuracy. Underpinning it all are the robust networks and data repositories required to seamlessly build and maintain awareness and understanding.